THE AUTOMATION OF INTER-NETWORKED BANKING AND TELLER MACHINE OPERATIONS USING UNIVERSAL SUBSCRIBER IDENTIFICATION MODULES

Miss. Vinothini. A[1], Prof. K. Chandra Prabha[2]
[1]*P.G. Student, Computer Application Department, Alagappa Chettiar Government College of engineering & Technology*
[2]*Head of the Department, Computer Application Department, Alagappa Chettiar Government College of engineering & Technology*

***Abstract*- Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week. This based on the facial recognition and also the multilevel security system based to work this entire concept. Here, we have some PHP support to analyze the person authorized identification. The proposed system is designed on the basis of mobile SIM and the face-recognition technique i.e. image will be capture with the help of camera placed in the design.**

***Index Terms*— ATM, inner networked atm, atm id**

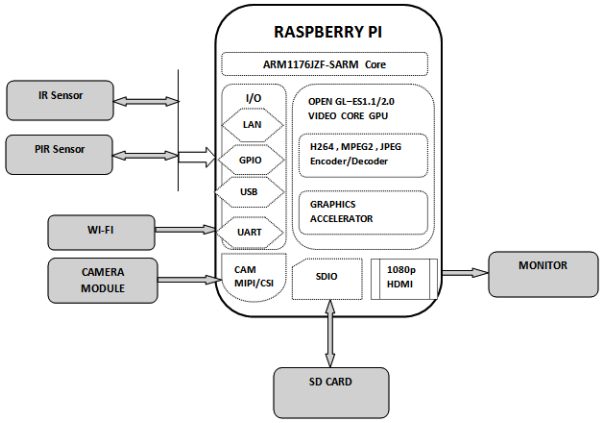
I. INTRODUCTION

Nowadays, banking sector is one of the most important parts of a human day to day life. Banking facilities are widely used by people for their economies activities. Automatic Teller Machine (ATM) is an electronic machine which is used for accessing a bank account from anywhere without the help of bank staff. The user can perform several banking activities like cash withdrawal, money transfer with the help of ATM. It is observed that the number of crimes related to ATM is increased hence there is a necessity to provide enhances security to ATM machine. Previous technologies provide security to transactions for identification of authorized user. But this is limited for secure transactions with ATM machine. Previous works focused on biometric technique to provide enhanced security to ATM transaction whereas GSM based technique is also implemented for the same purpose. Whereas, some system uses a combination of the both techniques Currently, ATM security is given to the transactions only.

GSM based security is provided in which One Time Password (WEBPAGE REQUEST) is send to registered number for transaction. The combination of GSM and RFID technology is also used which makes the system secure than only RFID technology. This technology has drawback so, biometric technology is introduced for ATM transaction. In biometric method fingerprint and face recognition system are used for ATM transaction. Fingerprint recognition system for ATM Transaction is used because each customer has unique fingerprints. So this system provides more secure transaction than GSM. Face recognition method is also used for security in which face is recognized from 3 angles for authentication purpose.Also, security is enhanced & facial recognition features. In this system, current face image matched with stored image and after matching the images correctly, request will be send to registered number user have to enter the webpage request number for completing transaction. There are many systems available for securing transactions, but there is no particular system to secure ATM machine.

So there is a necessity to implement a system which monitors and control the room where ATM machines are placed. The design of proposed system is divided into two parts. The first consists of a fingerprints reader placed at the entrance of ATM machine used to identify the user is authorized. The second part consists of Raspberry Pi module which is placed inside ATM centre for capturing real-time video and controlling purpose. This Anti-theft system ensures safe environment for card holders right from initial transaction to the end. It maintains communication channels with all the relevant national and international security working groups focused on the detection and prevention of crime, either directly against ATMs, or indirectly against ATMs through crimes perpetrated at other terminals.

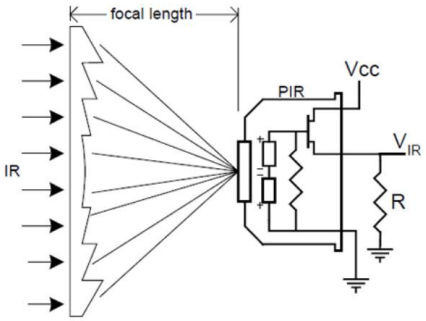
II.SYSTEM ARCHITECTURE



Automatic top rolling shutters are used if thief tries to break the sliding door to run way from ATM, GPS is used to track and get the location coordinates. Finger print scanner and RFID are used for authorizing bank personnel. Camera is installed for security recording. Buzzer is employed for alerting in case of theft. The cash drawer is equipped with a contact switch which gives feedback when the drawer is opened or broken. Here we have the raspberry microcontroller. Inside that controller we have the some more software use of find face recognition to the person. We are using the OPENCV advance image processing software with the help of this we will find the face of the authorized person. At last we allowing to take money to that person. What block diagram say know means here, IR sensor, help of this we will find the persons entering that room or not, help of PIR sensor find the human in front of machine or not, at last help of camera take photo and find the authorized person. The Raspberry Pi is a credit card sized single-board computer with an open-source platform that has a thriving community of its own, similar to that of the audio.

It can be used in various types of projects from beginners learning how to code to hobbyists designing home automation systems. There are a few versions of the Raspberry Pi, but the latest version, has improved upon its predecessor in terms of both form and functionality. Higher-spec variant increases the Raspberry pi GPIO pin count from 26 to 40 pins. There are now four USB 2.0 ports compared to two on the Model B. The SD card slot has been replaced with a more modern push-push type micro SD slot. It consumes slightly less power, provides better audio quality and has a cleaner form factor. To get started you need a **Raspberry Pi 3 Model B**, a **5V USB power supply** of at least 2 amps with a **micro USB cable**, any standard USB keyboard and mouse, an **HDMI cable** and monitor/TV for display, and a micro SD card with the operating system pre-installed. This pinots diagram will help you get familiar with the layout of the board and get started in immersing yourself into your own passion projects.

III. WORKING PROCEDURE



OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. Being a BSD-licensed product, OpenCV makes it easy for businesses to utilize and modify the code. The library has more than 2500 optimized algorithms, which includes a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms. These algorithms can be used to detect and recognize faces, identify objects, classify human actions in videos, track camera movements, track moving objects, extract 3D models of objects, produce 3D point clouds from stereo cameras, stitch images together to produce a high resolution image of an entire scene, find similar

images from an image database, remove red eyes from images taken using flash, follow eye movements, recognize scenery and establish markers to overlay it with augmented reality, etc. OpenCV has more than 47 thousand people of user community and estimated number of downloads exceeding.

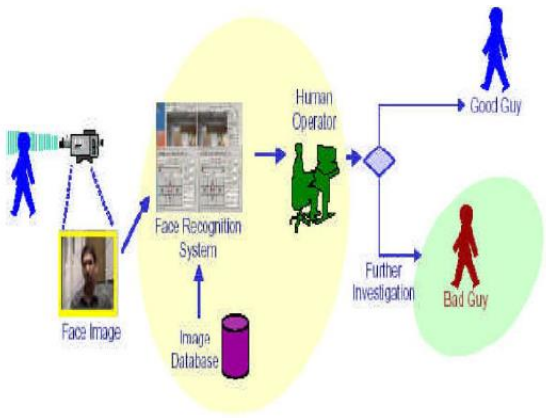
The library is used extensively in companies, research groups and by governmental bodies. Along with well-established companies like Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda, Toyota that employ the library, there are many startups such as Applied Minds, VideoSurf, and Zeitera, that make extensive use of OpenCV. OpenCV's deployed uses span the range from stitching streetview images together, detecting intrusions in surveillance video in Israel, monitoring mine equipment in China, helping robots navigate and pick up objects at Willow Garage, detection of swimming pool drowning accidents in Europe, running interactive art in Spain and New York, checking runways for debris in Turkey, inspecting labels on products in factories around the world on to rapid face detection in Japan. It has C++, C, Python, Java and MATLAB interfaces and supports Windows, Linux, and Mac OS. OpenCV leans mostly towards real-time vision applications and takes advantage of MMX and SSE instructions when available. A full-featured interfaces are being actively developed right now.

Now you'd say MATLAB also can do Image Processing, then why OpenCV? Stated below are some diferences between both. Once you go through them, you can decide for yourself. Matlab is built on Java, and Java is built upon C. So when you run a Matlab program, your computer is busy trying to interpret all that Matlab code. Then it turns it into Java, and then finally executes the code. OpenCV, on the other hand, is basically a library of functions written in C/C++. You are closer to directly provide machine language code to the computer to get executed. So ultimately you get more image processing done for your computers processing cycles, and not more interpreting. As a result of this, programs written in OpenCV run much faster than similar programs written in Matlab. So, conclusion? OpenCV is damn fast when it comes to speed of execution. For example, we might write a small program to detect peoples smiles in a sequence of video frames. In Matlab, we would typically get 3-4 frames analysed per second. In OpenCV, we would get at least 30 frames per second, resulting in real-time detection. Due to the high level nature of Matlab, it uses a lot of your systems resources. Matlab code requires over a gig of RAM to run through video. In comparison, typical OpenCV programs only require ~70mb of RAM to run in real-time. The difference as you can easily see is HUGE. **COST:** List price for the base (no toolboxes) MATLAB (commercial, single user License) is around USD 2150. **PORTABLITY:** MATLAB and OpenCV run equally well on Windows, Linux and MacOS. However, when it comes to OpenCV, any device that can run C, can, in all probability, run OpenCV.

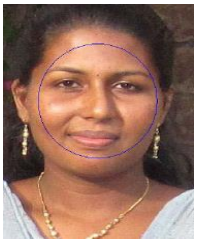
IV. FEASIBILITY STUDY

Feasibility study is made to see if the project on completion will serve the purpose of the organization for the amount of work, effort and the time that spend on it. Feasibility study lets the developer foresee the future of the project and the usefulness. A feasibility study of a system proposal is according to its work ability, which is the impact on the organization, ability to meet their user needs and effective use of resources. In the existing system the transactions are done only manually but in proposed system we have to computerize all the banking transaction using the software Online Banking. Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances as well as purchasing mobile cell phone prepaid credit. ATMs are known by various other names including automated banking machine, money machine, bank machine, cash machine, hole-in-the-wall, cashvpoint, Bancomat (in various countries in Europe and Russia), Multi banco (after a registered trade mark, in Portugal), and Any Time Money (in India).In the existing system the transactions are done only manually but in proposed system we have to computerize all the banking transaction using the software Online Banking. Thus when a new application is proposed it normally goes through a feasibility study before it is approved for development. The document provide the feasibility of the project that is being designed and lists various areas that were considered very carefully during the feasibility study of this project such as Technical, Economic and Operational feasibility.

V. IMAGE RECOGNITION VENDOR TEST

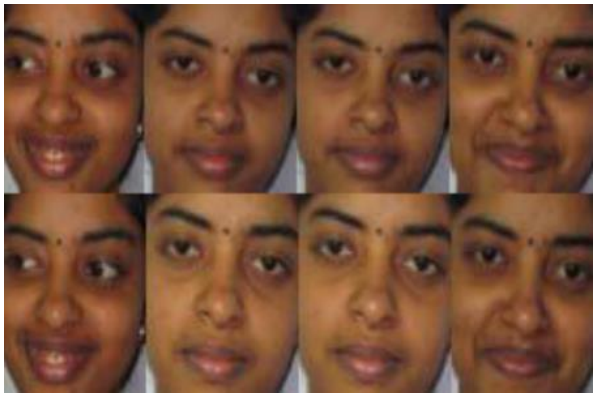


The medium size database consisted of number outdoor and video images from various sources. Figure 2 below gives an indication of the images in the database. The top row shows nodal position (red dots) for the images and bottom row shows the various poses of images. With the very good images from the large database (37,437 images) the identification performance of the best system at rank one is 96% at a false accept rate of 1%. OTP Algorithm In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments. Note that these factors must exist on both the mobile phone and server in order for both sides to generate the same password. Client and Server Database Design J2ME program is developed and installed on the mobile phone to generate the OTP. The program has an easyto-use GUI that is developed using the NetBeans drag and drop interface. The program can run on any J2ME-enabled mobile phone. The OTP program has the option of (1) generating the OTP locally using the mobile credentials, e.g. IMEI and IMSI numbers, or (2) requesting the OTP from the server via an SMS message. The default option is the first method which is cheaper since no SMS messages are exchanged between the client and the server. However, the user has the option to select the SMS-based method. In order for the user to run the OTP program, the user must enter his username and PIN and select the OTP generation method. The username, PIN, and generated OTP are never stored on the mobile phone.



The size of the database The Face Recognition Vendor Test (FRVT) has recognized the face recognition in four technical areas. They are high resolution still imagery, 3D facial scans, multi sample still facial imagery and pre-processing algorithm (PCA) that compensate pose and illumination. Individual's face The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). Here the part inside the oval is chosen and the other parts are rejected, artificial intelligence is used to simulate human interpretation of faces. Principal component analysis (PCA) involves a mathematical procedure which extracts facial features for recognition; this approach transforms face images into a small set of characteristic feature images called Eigen faces. The first principal component accounts for as much of the variability in the data as possible, and each succeeding component accounts for as much of the remaining variability as possible. These methods capture the local facial features and their geometric relationships.

They often locate anchor points at key facial features (eyes, nose, mouth, etc), connect these points to form a net and then measure the distances and angles of the net to create a unique face 'print'. SMS-Based Authentication System: In case the first method fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the one time password directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone.



The first step is the capturing of a face image. This would normally be done using a still or video camera. The face image is passed to the recognition software for recognition (identification or verification). This would normally involve a number of steps such as normalizing the face image and then creating a 'template' of 'print' to be compared to those in the database. The match can either be a true match which would lead to investigative action or it might be a 'false positive' which means the recognition algorithm made a mistake and the alarm would be cancelled. Each element of the system can be located at different locations within a network, making it easy for a single operator to respond to a variety of systems.

VI. CONCLUSION

Today, single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentications have recently been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is becoming a burden on both the client and organization. Since many clients carry a mobile phone today at all times, an alternative is to install all the software tokens on the mobile phone. This will help reduce the manufacturing costs and the number of devices carried by the client. Our paper has proposed a method of efficient 3D head tracking technique to overcome the consequence. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. Face recognition technology can be used worldwide to access buildings; however it can be used in ATMs, which would help address potential security threats in near future. Nowadays, most of the ATM has been attacked by the robberies. In this paper, a real-time monitoring system for ATM security based on accelerometer sensor, camera module, and fingerprint module is proposed.

VII. ACKNOWLEDGEMENT

This research was supported by my guide and supervisors. I thank my faculties and friends who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations of this paper. I thank **Mrs. Chandra Prabha. K**, Assistant Professor, Alagappa Chettiar Government College of Engineering & Technology for commenting that greatly improved the manuscript.

REFERENCES

[1] P. Thomas, B. Price, M. Petre, L. Carswell, and M. Richards, "Experiments with electronic examinations over the internet," in Proceedings for the 5th Computer Assisted Assessment (CAA) Conference, 2001. Available online: http://caaconference.co.uk/ pastConferences/2001/proceedings/q1.pdf.

[2] L. Parmer, "Helping students prepare for qualifying exams; a summary of WCRA Institute III," in Proceedings of the 8th Annual Meeting of the Western College Reading Association, Anaheim, CA, 1975.

[3] S. Görlich, Fundierung und Integration von E-Learning-Komponenten in die Präsenzlehre (in German), Ph.D. Thesis, University of Gießen, Faculty 06 – Psychology and Sports Science, Gießen, Germany, 2006.

[4] W.H. Dotson, J.B. Sheldon, and J.A. Sherman, "Supporting student learning: improving performance on short-essay exams using realistic practice opportunities," Journal of the Scholarship of Teaching and Learning, vol. 10(3), pp. 106-118, November 2010.

[5] I. Schagaev, N. Folic, N. Ioannides, and E. Bacon, "Multiple Choice Answers Approach: Assessment with penalty function for Computer Science and similar disciplines," International Journal of Engineering Education, vol. 28(6), pp. 1294-1300, 2012.

[6] E. Bacon, B.R. Kirk, G. Hagel, G. Kravtsov, M. Charnine, I. Schagaev, and R. Foggie, "Web-enhanced design of university curricula," in Proceedings of the 2013 International Conference on Frontiers in Education:

Computer Science and Computer Engineering (FECS), pp. 288-294.

[7] I. Schagaev, B. Kirk, and L. Bacon, "Essential knowledge aggregation, delivery, and assessment," ACM eLearn Magazine, May 2014.

[8] B. Jacobs, H. Bernd, and A. Fey, "Die Wirkung einer Probeklausur auf Klausurleistung und Angst in einer Statistikklausur" (in German). Available online at URN: urn:nbn:de:bsz:291-psydok-2720, July 2004.

[9] M. Peat and S. Franklin, "Supporting student learning: the use of computer-based formative assessment modules," British Journal of Educational Technology, vol. 33(5), pp. 515-523, November 2002.

[10] T. Deutsch, K. Herrmann, T. Frese, and H. Sandholzer, "Implementing computer-based assessment – a web-based mock examination changes attitudes," Computers & Education, vol. 58(4), pp. 1068-1075, May 2012.

[11] G.M. Novak, E.T. Patterson, A.D. Gavrin, and W. Gavrin, Just-in-Time Teaching: Blending active learning with web technology. Upper Saddle River, NJ: Prentice Hall, 1999.

[12] E. Mazur, Peer Instruction: A user's manual. Upper Saddle River, NJ: Prentice Hall, 1997.